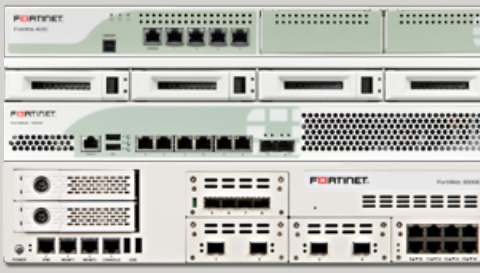
DATA SHEET

FortiWeb™
Web Application Firewall



FortiWeb

FortiWeb 100D, 400C, 1000D, 3000E and 4000E

Web Application Firewall

Web Applications are an Easy Target

Although Payment Card Industry Data Security Standards (PCI DSS) compliance is the main reason most organizations deploy Web Application Firewalls (WAFs), many now realize that unprotected web applications are the easiest point of entry for even unsophisticated hackers. Externally facing web applications are vulnerable to attacks such as cross site scripting, SQL injection, and Layer 7 Denial of Service (DoS). Internal web applications are even easier to compromise if an attacker is able to gain access to an internal network where many organizations think they're protected by their perimeter network defenses. Custom code is usually the weakest link as development teams have the impossible task of staying on top of every new attack type. However, even commercial code is vulnerable as many organizations don't have the resources to apply patches and security fixes as soon as they're made available. Even if you apply every patch and have an army of developers to protect your systems, zero day attacks can leave you defenseless and only able to respond after the attack has occurred.

Comprehensive Web Application Security with FortiWeb

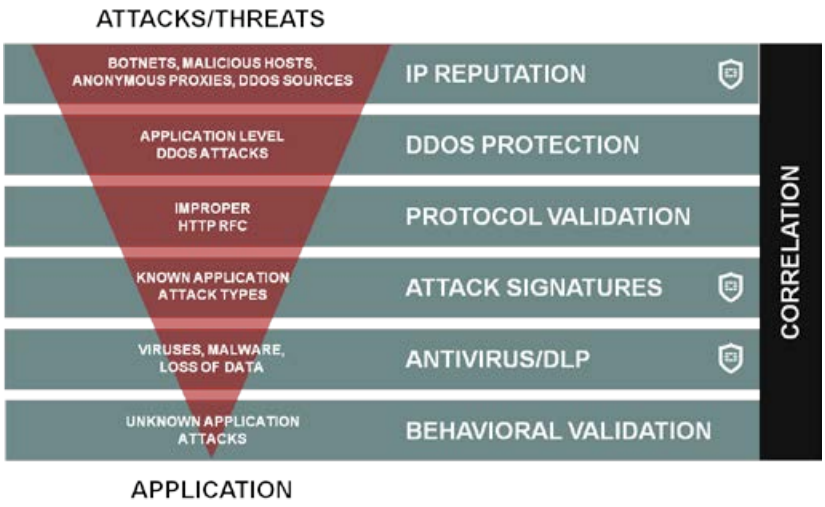
Using an advanced multi-layered and correlated approach, FortiWeb provides complete security for your external and internal web-based applications from the OWASP Top 10 and many other threats. Using IP Reputation services, botnets and other malicious sources are automatically screened out before they can do any damage. DoS detection and prevention keeps your applications safe from being overloaded by Layer 7 DoS attacks. FortiWeb checks that the request hasn't been manipulated using HTTP RFC validation. Requests are checked against FortiWeb's signatures to compare them against known attack types to make sure they're clean. Any files, attachments or code are scrubbed with FortiWeb's built-in antivirus and antimalware services. FortiWeb's auto-learning behavioral detection engine reviews all

A Complete Solution for Web Application Protection

- High-performance with up to 20 Gbps of throughput
- Included vulnerability scanner
- Included Layer 7 server load balancing
- Behavioral attack detection
- FortiGuard IP Reputation, Attack Signatures, and Antivirus
- Correlated, multi-layer threat scanning
- Integration with FortiSandbox for APT detection
- Transparent user validation for botnet protection
- Out-of-the-box protection against automated attacks
- Network and application layer DoS protection
- Authentication, site publishing and SSO
- Predefined known application protection

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

requests that have passed the tests for known attacks. If the request is outside of user or automatic parameters, the request is blocked. Lastly, FortiWeb provides a correlation engine where multiple events from different security layers are correlated to make a more accurate decision and help protect against the most sophisticated attacks. This combination provides near-100% protection from any web application attack, including zero day threats that signature file-based systems can't detect.



Included Vulnerability Scanning

Only FortiWeb includes a web application vulnerability scanner in every appliance at no extra cost to help you meet PCI DSS compliance. FortiWeb's vulnerability scanning dives deep into all application elements and provides in-depth results of potential weaknesses in your applications. Vulnerability scanning is always up-to-date with regular updates from FortiGuard Labs.

Blazing Fast SSL Offloading

FortiWeb is able to process up to tens of thousands of web transactions by providing hardware accelerated SSL offloading in most models. With near real-time decryption and encryption using ASIC-based chipsets, FortiWeb can easily detect threats that target secure applications.

Application Delivery and Authentication

FortiWeb provides advanced Layer 7 load balancing and authentication offload services. FortiWeb can easily expand your applications across multiple servers using intelligent, application-aware Layer 7 load balancing and can be combined with SSL offloading for load balancing secure application traffic. Using HTTP compression, FortiWeb can also improve bandwidth utilization and user response times for content-rich applications. Authentication offloading integrates with many authentication services including LDAP, NTLM, Kerberos and RADIUS with 2-factor authentication for RADIUS and RSA SecureID. Using these authentication services, you can easily publish websites and use Single Sign On (SSO) for any web application including Microsoft applications such as Outlook Web Access and SharePoint. Finally, FortiWeb can improve application response times by caching often-used content to serve it users faster than having to request the same information each time it is needed.

Secured by FortiGuard

Fortinet's Award-winning FortiGuard Labs is the backbone for many of FortiWeb's layers in its approach to application security. Offered as 3 separate options, you can choose the FortiGuard services you need to protect your web applications. FortiWeb IP Reputation service protects you from known attack sources like botnets, spammers, anonymous proxies, and sources known to be infected with malicious software. FortiWeb Security Service is designed just for FortiWeb including items such as application layer signatures, malicious robots, suspicious URL patterns and web vulnerability scanner updates. Finally, FortiWeb offers FortiGuard's top-rated antivirus engine that scans all file uploads for threats that can infect your servers or other network elements.

Deep Integration for Advanced Threat Protection

FortiWeb is one of many Fortinet products that provides integration with our FortiSandbox advanced threat detection platform. FortiWeb can be configured with FortiSandbox to share threat information and block threats as they're discovered in the sandboxing environment. Files uploaded to web servers can be sent to FortiSandbox for analysis. Alerts are sent immediately when malicious files are identified and future similar files are blocked immediately.

Virtual Patching

FortiWeb provides integration with third party vulnerability scanners to provide dynamic virtual patches to security issues in application environments. Vulnerabilities found by the scanner are quickly and automatically turned into security rules by FortiWeb to protect the application until developers can address it in the application code.

Central Management and Reporting

FortiWeb offers the tools you need to manage multiple appliances and gain valuable insights on attacks that target your applications. From within a single management console you can configure and manage multiple FortiWeb gateways using our VMware-based central management utility. If you need an aggregated view of attacks across your network, FortiWeb easily integrates into our FortiAnalyzer reporting appliances for centralized logging and report consolidation from multiple FortiWeb devices.

FEATURES/HIGHLIGHTS

Deployment options

- Reverse Proxy
- Inline Transparent
- True Transparent Proxy
- Offline Sniffing

Web Security

- Automatic profiling (white list)
- Web server and application signatures (black list)
- IP Reputation
- IP Geolocation
- HTTP RFC compliance

Application Attack Protection

- OWASP Top 10
- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Built-in Vulnerability Scanner
- Third-party scanner integration (virtual patching)

Security Services

- Web services signatures
- XML protocol conformance
- Malware detection
- Virtual patching
- URL rewriting
- Cookie poisoning protection
- Custom error message and error code handling
- Operating system intrusion signatures
- Known threat and zero-day attack protection
- DoS prevention
- Advanced correlation protection using multiple security elements
- Data leak prevention
- Web Defacement Protection

Application Delivery

- Layer 7 server load balancing
- HTTPS/SSL Offloading
- HTTP Compression
- Caching

Authentication

- Active and passive authentication
- Site Publishing and SSO
- RSA Access for 2-factor authentication
- LDAP and RADIUS support
- SSL client certificate support

Management and Reporting

- Web user interface
- Command line interface
- Central management for multiple devices
- REST API
- Centralized logging and reporting
- Real-time dashboards
- Bot dashboard
- Geo IP Analytics
- SNMP, Syslog and email Logging/Monitoring
- Administrative Domains with full RBAC

Other

- IPv6 Ready
- High Availability with Config-sync for syncing across multiple active appliances
- Auto setup and default configuration settings for simplified deployment
- Pre-configured for common Microsoft applications; Exchange, SharePoint, OWA

ORDER INFORMATION

Product	SKU	Description
FortiWeb 100D	FWB-100D	Web Application Firewall — 4x GE RJ45 ports, 16 GB storage.
FortiWeb 400C	FWB-400C	Web Application Firewall — 4x GE RJ45 ports, 1 TB storage.
FortiWeb 1000D	FWB-1000D	Web Application Firewall — 2x GE SFP slots, 6x GE RJ45 ports (includes 4x bypass ports), dual AC power supplies, 4 TB storage.
FortiWeb 3000E	FWB-3000E	Web Application Firewall — 4x GE RJ45 ports, 4x GE RJ45 bypass ports, 4x GE SFP ports, 4x 10G SFP+ ports, dual AC power supplies, 2x 2 TB storage.
FortiWeb 4000E	FWB-4000E	Web Application Firewall — 4x GE RJ45 ports, 4x GE RJ45 bypass ports, 4x GE SFP ports, 4x 10G SFP+ ports, dual AC power supplies, 2x 2 TB storage.
FortiWeb-VM01	FWB-VM01	FortiWeb-VM, up to 1 vCPU supported. 64-bit OS.
FortiWeb-VM02	FWB-VM02	FortiWeb-VM, up to 2 vCPUs supported. 64-bit OS.
FortiWeb-VM04	FWB-VM04	FortiWeb-VM, up to 4 vCPUs supported. 64-bit OS.
FortiWeb-VM08	FWB-VM08	FortiWeb-VM, up to 8 vCPUs supported. 64-bit OS.
Central Manager 10	FWB-CM-BASE	FortiWeb Central Manager license key, manage up to 10 FortiWeb devices, VMware vSphere.
Central Manager Unlimited	FWB-CM-UL	FortiWeb Central Manager license key, manage unlimited number of FortiWeb devices, VMware vSphere.

SPECIFICATIONS

	FORTIWEB 100D	FORTIWEB 400C	FORTIWEB 1000D	FORTIWEB 3000E	FORTIWEB 4000E
Hardware					
10/100/1000 Interfaces (RJ-45 ports)	4	4	6 (4 bypass) 2x SFP GE (non-bypass)	8 (4 bypass), 4x SFP GE (non-bypass)	8 (4 bypass), 4x SFP GE (non-bypass)
10G BASE-SR SFP+ Ports	0	0	0	4	4
USB Interfaces	2	1	2	2	2
Storage	16 GB	1 TB	2x 2 TB	2x 2 TB	2x 2 TB
Form Factor	Desktop	1U	2U	2U	2U
Power Supply	Single	Single	Dual Hot Swappable	Dual Hot Swappable	Dual Hot Swappable
System Performance					
Throughput	25 Mbps	100 Mbps	1 Gbps	5 Gbps	20 Gbps
Latency	Sub-ms	Sub-ms	Sub-ms	Sub-ms	Sub-ms
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	0	32	64	64	64
All performance values are "up to" and vary depending on the system configuration.					
Dimensions					
Height x Width x Length (inches)	1.61 x 8.27 x 5.24	1.7 x 17.1 x 14.3	3.50 x 17.24 x 14.49	3.5 x 17.5 x 22.6	3.5 x 17.5 x 22.6
Height x Width x Length (mm)	41 x 210 x 133	44 x 435 x 364	88 x 438 x 368	88 x 444 x 574	88 x 444 x 574
Weight	2.3 lbs (1.1 kg)	14.15 lbs (6.42 kg)	27.6 lbs (12.5 kg)	56.2 lbs (22.5 kg)	56.2 lbs (22.5 kg)
Rack Mountable	Optional	Yes	Yes, with flanges	Yes	Yes
Environment					
Power Required	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Maximum Current	110V/1.2A, 220V/1.2A	120V/4A, 240V/2A	100V/5A, 240V/3A	120V/2.6A, 240V/1.3A	120V/3A, 240V/1.5A
Power Consumption (Average)	18 W	100.3 W	115 W	200 W	248.5 W
Heat Dissipation	74 BTU/h	410.7 BTU/h	471 BTU/h	1045.5 BTU/h	1219.8 BTU/h
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
Storage Temperature	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)	-13–158°F (-25–70°C)
Humidity	10–90% non-condensing	10–90% non-condensing	5–95% non-condensing	5–95% non-condensing	5–95% non-condensing
Compliance					
Safety Certifications	FCC Class A Part 15, C-Tick, VCCI, CE, UL/cUL, CB	FCC Class A Part 15, C-Tick, VCCI, CE, UL/cUL, CB	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE	FCC Class A Part 15, UL/CB/cUL, C-Tick, VCCI, CE

	FORTIWEB-VM (1 vCPU)	FORTIWEB-VM (2 vCPU)	FORTIWEB-VM (4 vCPU)	FORTIWEB-VM (8 vCPU)
System Performance				
HTTP Throughput	25 Mbps	100 Mbps	500 Mbps	2 Gbps
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	4 to 64 based on the amount of memory allocated			
Virtual Machine				
Hypervisor Support	VMware ESX / ESXi 4.0 / 4.1 / 5.0 / 5.1 / 5.5 / 6.0, Microsoft Hyper-V, Citrix XenServer 6.2, Open Source Xen 4.2, Amazon Web Services (AWS), KVM			
vCPU Support (Minimum / Maximum)	1	2	2 / 4	2 / 8
Network Interface Support (Minimum / Maximum)	1 / 4 (10 VMware ESX)	1 / 4 (10 VMware ESX)	1 / 4 (10 VMware ESX)	1 / 4 (10 VMware ESX)
Storage Support (Minimum / Maximum)	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB
Memory Support (Minimum / Maximum)	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit	1,024 MB / Unlimited for 64-bit
Recommended Memory	4 GB	4 GB	4 GB	4 GB
High Availability Support	Yes	Yes	Yes	Yes

Actual performance values may vary depending on the network traffic and system configuration. Performance metrics were observed using a Dell PowerEdge R710 server (2x Intel Xeon E5504 2.0 GHz 4 MB Cache) running VMware ESXi 5.5 with 4 GB of vRAM assigned to the 4 vCPU and 8 vCPU FortiWeb Virtual Appliance and 4 GB of vRAM assigned to the 2 vCPU FortiWeb Virtual Appliance.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480